United States Department of Agriculture
Marketing and Regulatory Programs
Animal and Plant Health Inspection Service

Directive **APHIS 3120.3** **7/31/07**

APPROVAL OF SOFTWARE ON APHIS-OWNED COMPUTERS

1. PURPOSE

This Directive establishes APHIS policy for approval of software installed on APHIS-owned computers.

2. REFERENCES

a. APHIS Directive 3140.4, APHIS Desktop Computer Security Policy, dated 2/22/06. http://www.aphis.usda.gov/library/directives/pdf/aphis3140_4.pdf

b. APHIS Software Standards. https://data01.aphis.usda.gov/it/itsec.nsf

3. SCOPE

a. This Directive applies to all APHIS-owned computers and their users, including desktops, laptops, tablets, and servers.

b. This Directive does not apply to:

(1) Telecommunication devices such as routers and switches;

(2) Communication devices such as cell phones, personal digital assistants (PDAs), and telephones; or

(3) Peripherals such as printers.

4. DEFINITIONS

a. Desktop computer. Any computer whose operating system is a desktop operating system, e.g., Windows 2000, Windows XP, or Windows Vista. This includes all form factors (rackmount, tower, small form factor, tablet, laptop).

b. Server. Any computer whose operating system is a server operating system, e.g., Windows 2000 Server, Windows 2003 Server, Unix/AIX. This includes all form factors (rackmount, tower, small form factor, tablet).

c. Mandatory Software. Software required to be installed on the computer, usually for security reasons (e.g., antivirus client, patch deployment software, etc.).

d. Standard Software. Software that is typically installed on Agency servers or desktop computers as part of the Agency standard baseline configuration.

e. Approved Software. Software which meets one of the following criteria:

(1) Software identified in 2.b. above as Mandatory or Standard Software.

(2) Program-specific software approved by this Directive.

(3) Software for which the user has an approved Desktop Security Exception Request (DSER) per the terms of this Directive.

f. Program-specific software. Non-mandatory, non-standard software required by APHIS program units.

g. Desktop Security Exception Request (DSER). The process by which a request for exception to APHIS system configuration requirements is submitted for review and approval by the Chief Information Officer. http://www.aphis.usda.gov/library/forms/pdf/aph144.pdf

h. APHIS Software Standards**.** This document defines:

(1) Standard software for APHIS desktop computers and servers.

(2) Mandatory software for APHIS desktop computers and servers.

(3) Forbidden software for APHIS desktop computers and servers.

5. POLICY

APHIS supports and enforces a policy of secure computing, which helps ensure the continuing ability of all APHIS program units to fully support the APHIS mission. Approved computer configuration, including installed software, is a recognized information security best practice, and an important component of the Agency's computer security strategy. Employee awareness and adoption of security best practices in this area are an important cornerstone of the Agency's security plan, and as such:

a. All software installed on APHIS computers will be approved software.

b. Approved software must meet the following criteria. Program units must follow this section as a checklist for approving Program-specific software. Software must:

(1) Be owned by APHIS. (Personally-owned software may not be installed).

(2) Be installed for the purpose of performing official APHIS business.

(3) Not interfere with the installation, upgrade, or operation of mandatory or standard software.

(4) Be secure. The security of the installed software will be ascertained by scanning the system with the Agency scanning software. If no vulnerabilities are detected, the software will be considered to be secure.

(5) Be legally licensed and used in accordance with the license agreement.

(6) Not be identified as forbidden in the APHIS Software Standards.

(7) Not consume a disproportionate amount of bandwidth and/or cause general network slowdown.

c. Software which is required to make a hardware component operational is automatically approved.

d. If a Standard Software is identified in the APHIS Software Standards for a software category, any deviation from that standard requires an approved DSER.

e. Exceptions to the terms of this Directive must be approved in writing. The Desktop Exception Request form and process will be used to submit such requests (for both desktops and servers).
http://www.aphis.usda.gov/library/forms/pdf/aph144.pdf

6. RESPONSIBILITIES

a. The APHIS Chief Information Officer, Information Technology Division (ITD), will:

(1) Approve and ensure implementation of this Directive.

(2) Approve any modifications to this Directive.

b. Deputy Administrators/Directors of Program Units, and Heads of Major Business Offices will:

(1) Disseminate this Directive to their respective staffs.

(2) Ensure that the terms of this Directive are followed within their program units.

(3) Assist in promptly identifying, investigating, and rectifying violations of this Directive.

c. The APHIS Information Systems Program Manager (ISSPM); MRPBS, ITD, Customer Service Branch (CSB) Manager; MRPBS, ITD, Technical Resource Management (TRM) Manager; will:

(1) Provide content for the APHIS Software Standards.

(2) Design and implement an educational program for both new and existing employees to ensure awareness of the terms of this Directive.

(3) Design and implement a program for monitoring Agency computers for compliance with the terms of this Directive.

(4) Work with the program units to bring noncompliant computers and their users into compliance. In cases of continued non-compliancy:

(a) Take appropriate measures to deny APHIS network and resource access to computers not compliant with this Directive.

(b) Report incidents of noncompliance with this Directive to the appropriate Deputy Administrator for rectification.

d. The MRPBS, ITD, Policy, Planning and Training (PPT) Staff Manager, will:

(1) Maintain this Directive, including receiving requests for, and executing, modifications in response to change requests and/or new requirements.

(2) Be responsible for maintenance of the APHIS Software Standards, including:

(a) Requests for modification.

(b) Requests for modification and/or new requirements within 30 days of request or notification of new requirement.

(c) A forum for discussion among all program units and appropriate members of MRPBS, ITD, of proposed changes prior to approval.

(d) Notification all IT employees of changes within 14 days of the change.

(e) Publication in a centrally and electronically accessible location.

e. The Information System Security Manager (ISSM) for each Program Unit will:

(1) Review, approve, and maintain documentation of Program-specific software.

(2) Review, provide recommendation for approval or denial of, and maintain records of, all DSERs originating from his/her program unit.

f. Agency Computer Support Employees will:

(1) Comply with the terms of this Directive when configuring APHIS computers.

(2) Take immediate corrective action to bring computer configurations into conformance with the terms of this Directive or obtain an approved APHIS DSER for nonconforming software for computers under their care.

(3) Assist in promptly identifying, investigating, and rectifying violations of this Directive.

(4) Assist users in understanding the terms of this Directive, the reasons for its implementation, and the importance of compliance with its terms to ensure a secure computing environment for all employees.

(5) Proactively review and provide recommendations for modifications to this Directive and the APHIS Software Standards, to support the needs of program unit employees and the APHIS mission.

g. APHIS employees will:

(1) Comply with the terms of this Directive.

(2) Ensure that any APHIS-owned desktop computer which they use, or for which they have support responsibility, conforms to the terms of this Directive or obtain an approved DSER for nonconforming software.

7. INQUIRIES

a. Questions concerning the information and processes described in this Directive should be directed to the MRPBS, ITD, CSB Manager.

b. This Directive can be accessed via the Internet APHIS website at ***www.aphis.usda.gov/library***

/s/
Gregory L. Parham
APHIS Chief Information Officer